Published and Copyright (c) 1999 - 2013
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1507 02/15/13

~ Valentine’s Day Scams! ~ People Are Talking! ~ Facebook Gets Hacked?
~ Google Is Sharing Info ~ Adobe Security Bug! ~ Steam for Linux!
~ "Google for Spies"! ~ Crashproof Computer? ~ Egypt’s YouTube Ban!

~ MacBook Pro Price Cuts ~ Fake Names Ban Fight! ~ Employee Privacy!

-* Bushnell Book on Steve Jobs! *-
-* Spain Nabs Ransomware Cybercrime Gang *-
-* Medals for Drone Strokes and Cyberattacks? *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

It was a blizzard, aptly named the Blizzard of 2013, and it was one for the record books. The storm, as I mentioned briefly last week, started last Friday night and ended some time on Saturday. For my immediate area, we had an average of a little over two feet of wind-swept snow. Some areas received much more, and some over three feet! For all practical purposes, New England was shut down to everything but snow-removal equipment. Here it is, a week later, and many areas throughout New England are still dealing with some problems due to all of the wind and snow.

It took us over five hours, with two snow throwers and shovels, to clear what we had to clean. That was on Saturday. On Sunday, we spent another hour or so doing what we could to clean the snow from our roofs. The forecast called for rain a day later, so we wanted to play it safe. The ban on road travel was finally lifted late Saturday afternoon, but most people stayed at home to continue the clean-up.

Hopefully, any of you, our readers, caught up in this weather managed to make it through the storm relatively unscathed. Things are starting to get back to normal now, especially with the aid of some nice weather the past few days - sunshine and warm temperatures. No idea how long the reprieve will last!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Steam for Linux Now Available!
""""""""""""""""""""""""""""""""""" Rough Tides for The Wii U!
Bushnell Book on Steve Jobs!
And much more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

Steam for Linux Now Available

Valve, creators of best-selling game franchises (such as Counter-Strike and Team Fortress) and leading technologies (such as Steam and Source), announced the release of its Steam for Linux client. In celebration of the release, over 50 Linux titles are now 50-75% off until Thursday, February 21st at 10 AM PST.

The Steam client is now available to download for free from the Ubuntu Software Center. Ubuntu is the most popular distribution of Linux used by millions of people globally and known for its well-designed, easy-to-use customer experience.

The introduction of Steam to Ubuntu demonstrates growing demand for open systems from gamers and game developers, said David Pitkin, Director of Consumer Applications at Canonical. We expect a growing number of game developers to include Ubuntu among their target platforms. We re looking forward to seeing AAA games developed with Ubuntu in mind as part of a multi-platform day and date release on Steam.

We re huge fans of Linux. It s like the indie OS a perfect home for our indie game, said Alen Ladavac, CTO of Croteam, creator of the Serious Sam franchise of games. And who better to lead the charge into Linux gaming than Valve? With Steam distribution on Windows, Mac OS, and now Linux, plus the buy-once, play-anywhere promise of Steam Play, our games are available to everyone, regardless what type of computer they re running. That s huge.

Team Fortress 2, the Free to Play game, is also now available on Steam for Linux. For a limited time, Steam users who play the game on Linux will automatically receive a free, exclusive in-game item: Tux, the Linux mascot, can be carried by any of the game s classes and traded between players. Additional Valve titles available on Steam for Linux include Half-Life, Counter-Strike 1.6, and Counter-Strike: Source.

In addition to games, the Steam for Linux client includes Big Picture, the new mode of Steam designed for use with a TV and game controller. With Steam for Linux and Big Picture mode, Valve anticipates a growing number of gamers will use Steam in the living room.

Steam is a leading platform for the delivery and management of PC and Mac games with over 50 million accounts around the world and over 2,000 titles offered. More details regarding Steam for Linux, including community discussion, official announcements and syndicated news can all be tracked on the Steam for Linux Community Hub at http://steamcommunity.com/linux.

January Sales Show Continued Rough Tides for The Wii U

The NPD Group has released its U.S. video game retail estimates for January 2013, but they require a little bit of explanation.

The NPD’s reporting schedule aligns with the National Retail Federation’s,

including its "leap week", which happened to fall on this January's monthly calendar.

So when we say that video game retail sales jumped 9 percent in January, that's not a fair comparison: January 2013 was a five-week month, whereas January 2012 was only four.

With some simple math to adjust for the difference and estimate what a four-week January would have been, overall new retail sales across hardware, software and accessories is down an estimated 13 percent, from $765.6 million in January 2012 to roughly $667.8 million in January 2013.

While the NPD no longer provides specific sales numbers for hardware, a representative does tell us that sales of the Wii U hardware for its first three months on the market are down 38 percent from what the Wii's numbers were at that same point.

We're told by someone with access to the NPD's data that sales for January were "well under" 100,000 units. By our estimates, sales were somewhere between 45,000 and 59,000 units for the month, which is lower than any of the three previous-generation home consoles sold in their worst months, with the possible exception of a recent performance by the original Wii.

Similarly, we don't know any software sales numbers, but from NPD's report we can see where Wii U SKUs of multiplatform games compare to other SKUs, and it doesn't look good.

In instances where a game exists on both the Wii and the Wii U (Just Dance 4, NBA 2K13, Madden NFL 13, Skylanders Giants and FIFA Soccer 13), the Wii version came out on top every time. In Madden's case, it was even outsold by the portable version for Sony's ailing Vita handheld.

Top 10 software chart (SKUs combined)
1. Call of Duty: Black Ops II (360, PS3, Wii U, PC)
2. Far Cry 3 (360, PS3, PC)
3. Just Dance 4 (Wii, 360, PS3, Wii U)
4. NBA 2K13 (360, PS3, Wii, Wii U, PSP, PC)
5. Madden NFL 13 (360, PS3, Wii, PSV, Wii U)
6. DMC: Devil May Cry (PS3, 360)
7. Halo 4 (360)
8. Assassin's Creed III (360, PS3, Wii U, PC)
9. Skylander Giants (Wii, 360, PS3, 3DS, Wii U)
10. FIFA Soccer 13 (PS3, 360, PSV, Wii, Wii U, 3DS, PSP)

Next-generation PlayStation 4 Controller Leaks

An image published by Destructoid on Thursday supposedly revealed a prototype of the controller for Sony s (SNE) upcoming PlayStation 4 gaming console. The device pictured looks like a traditional PlayStation controller with a directional pad, two analog sticks and four buttons, but it also includes a small touchpad and a blue light that resembles Sony s PlayStation Move motion device. The controller was said to be one of the prototypes that Sony tested for its next-generation console. The story was later confirmed by sources speaking to Kotaku who said the photo is the real deal, but it may not represent the final form of the controller.

A second image was posted on the forums at GameTrailers on Friday that

revealed a 3.5-millimeter headphone jack at the bottom of the controller and slightly longer handles than the original image.

Recent reports have suggested that the system will be equipped with an 8-core AMD processor, 8GB of RAM, 160GB of internal storage, a Blu-ray drive and be capable of running 3D games at 60 frame-per-second at a full HD 1080p resolution.

Sony is scheduled to hold a press conference on February 20th in New York City where it is expected to unveil the PlayStation 4 BGR will be reporting live from the event.

Stop Blaming Video Games for America’s Gun Violence

Studies show that a child playing a violent video game does not necessarily increase the likelihood that he or she will engage in real violence. Americans need to stop blaming something other than our own behaviors and ideologies for societal violence, especially gun violence.

Recently, America s attention has been understandably focused on the potential causes of increased violence especially gun violence particularly among children and youth, and how to stop it. Alongside gun-control proposals, some of which President Obama is likely to highlight in his State of the Union address tonight, much of that attention has looked at the potential of violent video games to cause or exacerbate the tendencies of youth to engage in real, harmful violence.

While I applaud increased vigilance on the part of parents in supervising their children s behaviors and pastimes, a child playing a violent video game does not necessarily increase the likelihood that he or she will engage in real violence at that age or later in life.

Various reports and commentaries have documented the fact that Sandy Hook shooter Adam Lanza s video game playing included violent shooter games like Call of Duty, Counterstrike, and Starcraft. Some have cited that activity as a possible cause for his shooting massacre.

But if Lanza was playing Call of Duty 4, he was one of millions. On the Xbox 360 console alone, the game s developer, Infinity Ward, has documented nearly 4.4 million online players, not counting players who use a PlayStation 3 or aren t online. The statistics for Counterstrike are similar an estimated 62,142 per day. And Starcraft is so popular in Korea, that it has professional leagues and an estimated online player population of around 50,000 each day.

Of those millions of players, few commit an act of violence, certainly not enough to say that, statistically, video game play is a principle cause or even a significant cause of real-world violent behavior.

So why are so many people blaming the video game industry?

It s a phenomenon known as cultural lag, and it s what causes us to be hesitant in adopting new technologies, trying new fads, and changing our social mores. Cultural lag can be a good thing some new things are dangerous, come with high levels of risk, and can infinitely do more harm than good. But cultural lag also can inhibit the development of technologies and society because of irrational fears, which is what I m

seeing with recent criticism of the gaming industry.

Before video games, society blamed rock n roll for violence and bad behavior among young people. Before rock n roll, we blamed television. Before television, movies. Before movies, mystery novels, which were once known as penny dreadfuls. Before mystery novels, Shakespeare, who repeatedly was accused of producing violent, lecherous, and otherwise improper behavior in his audience.

In essence, as a society, we always will try to find out why bad things happen, but we aren t actually very good at finding the answers. We look back at our past with rose-colored glasses and look forward into the future with trepidation.

We see our own childhoods as joyful and carefree, and when, as adults, we are exposed to the grim realities of our world, we wonder, What happened? . And then we try to explain the difference between the past that we remember and the present as we perceive it. When we do this, we very often look to technologies that did not exist 20, 30, or 40 years ago, and we think: That didn t exist back then when things were better, therefore it must have some impact on why things have gotten worse now.

First of all, I am unconvinced that things have gotten worse, but even if we assume that they have, in blaming technologies like video games for real-life violence, we assume causation, where numerous studies show there is only correlation at best. This is tantamount to assuming, as journalist Jeanine Celestin-Greer of Gamastura (a gaming journalism website) points out, that because Lanza drank Mountain Dew, Mountain Dew causes violent behavior.

In a recent article in The Chronicle of Higher Education, Christopher J. Ferguson, a psychologist at Texas A&M International University, claimed that the recent outcry against video games as the cause of school shootings in general is patently fallacious. He explains that among hundreds of studies on violence and video games, not a single one has proven conclusively a causal relationship between violent behaviors in the real world and violent video-game play. And yet, scholars and politicians who often have little to no experience playing video games themselves continue to suggest that this is the case.

Americans need to stop trying to blame something other than ourselves for the increase if there is an increase in violent behavior.

Video games, music, television, movies, novels, and Shakespeare don t cause violence. Mental illness, psychological abuse, and physical abuse cause violence. Ideologies that reward and condone aggression, particularly in men, cause violence. Global genocide causes violence. The only conclusive evidence we do have is that it is real-life violence that causes real-life violence.

As long as we, as a society, condone violence in the name of nationalism, continue to minimize domestic violence and rape, and promote aggression as ideal masculinity, violence will continue to be a problem in our homes, on our streets, and in our schools. Critics will argue that the imagery and plots of video games do just that and in turn, perpetuate those behaviors. Yes, video games reflect some of these highly problematic aspects of our society that contribute to a tolerance of violence. Just like movies and books. But they don t cause it.

Remove video games from the equation and you will still have a commensurate

level of violence.

And yes, video games can influence ideology, but they aren't the only or even the predominant influence on society or an individual. In fact, video games can influence our ideologies in as many if not more positive ways than they do negative ones. Many recent games actually encourage players to play non-violently and reward players for humane treatment and good judgment.

So while video games are influencing us, and sometimes through violent images and play, many of them are pushing us to criticize the very violence that some people seem to believe they are causing.

The dialogue we need to have is about real violence, not virtual violence, and I sincerely hope that America s leaders recognize this as we move forward in addressing the problem.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

Atari Founder's Book on Steve Jobs To Kick Off New Publishing Platform

In 1975, Nolan Bushnell was riding high. He'd just co-founded Atari and launched the world's first home video game, Pong. And then there was the oddball engineer he'd hired, Steve Wozniak, who'd brought his equally odd friend Steve Jobs to work with him for free. "Great," Bushnell thought. "Two for the price of one."

It wasn't until 2012 that Bushnell sat down to write the whole story: how Jobs and Wozniak offered him a third of Apple for $50,000 and he turned it down; how he stayed a friend and advisor to the growing company over the years; and most importantly, what you can learn from the whole experience. "It's less of a biography and more of a book on creative infrastructure," Bushnell tells Mashable.

But when he tried to find an outlet for the book, How to Find the Next Steve Jobs, Bushnell got frustrated with the traditional publishing houses. It would take up to four years to edit it and publish it, they said. "I don't have that kind of time," replied Bushnell, now 70. He also didn't accept that publishers should keep 80% or more of the book's sales, as is traditional.

So Bushnell turned to Net Minds, a brand new publishing platform that officially launched Wednesday. Net Minds is the brainchild of Tim Sanders, a former Yahoo executive and the New York Times bestselling author of Love is the Killer App. It will publish regular books as well as e-books, and lets authors build a team to edit, design and market the book in exchange for a cut of the sales.

Sanders' founding principle: books should be run like startups. "The industry is incredibly inefficient at every level," he tells Mashable.

"Frankly, for a lot of authors, it’s incredibly unfair. Advances are dropping. And there’s no reason why it should take three years to publish."

Net Minds has built software that can turn a document into a printed galley copy (used by authors to check for mistakes) in just three days, rather than the usual few months. Flipping the traditional royalty model on its head, the startup keeps 20% of all book sales. The author gets 80% (or 90% in Bushnell’s case), and gets to apportion that as he or she sees fit. The startup says it will connect authors to freelance editors, designers, marketers and PR folks to get them going.

Bushnell opted to keep 50% of the sales, and give the rest to his creative team. "I like everyone to have a little skin in the game," he says. The book, Net Minds’ first, will go on sale in bookstores and online in mid-March.

Whether the business model will work remains to be seen. We’re a little skeptical at the idea that editors, designers, marketers and book PR people will essentially work for the promise of future book royalties with nothing up front. (Net Minds says authors can also choose to fund their team out of their own pockets, and that one has already used a crowdsourced fundraising platform to do so.)

We also wonder if authors weaned on the notion of getting an advance will want to switch to a royalty-only system, even if they get to keep 80%.

Either way, Net Minds says it has acquired another 20 book projects and is soliciting more. "We’re not just for traditional authors," Sanders says. "We’re for emerging authors." Most authors are writing their books part-time now anyway, he says; why not skip the advance for the promise of massive royalties?

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Pentagon To Start Awarding Medals for Drone Strokes and Cyberattacks

The Defense Department is reportedly inventing a new medal designed to reward soliders who fight battles from the safety of their computer consoles. The Associated Press says the Pentagon is creating a new ribbon, called the Distinguished Wardfare Medal that will be given for "extra achievement" related to a military operation. That would include drone pilots operating unmanned planes from halfway around the world, or even hackers who launch a successful cyberattack on an enemy. Unlike all other combat-related medals, this would be the first one that you can be awarded without actually putting your life online.

While the move will undoubtedly rankle some of the infantrymen and Special Forces veterans who get shot at on a near daily basis during their combat

deployments, the Pentagon is eager to find some way to recognize the achievements of those who are fighting modern battles, but just happen to be doing so from a computer lab or flight simulator instead of the war zone. Since a growing number of military operations don't actually call on soldiers, sailors, or pilots to risk their lives anymore, the Armed Forces are not handing out as many of their more traditional combat medals as they used. Despite being perpetually at war since 2001, there have only been 10 Medals of Honor given out since the September 11 attacks, and the number of Navy and Air Force Crosses awarded has actually declined.

Yet a successful drone pilot creating air cover for a squadron on the ground can save just as many lives as one who takes a bullet for fellow solider. That's not the same level of heroism, obviously, but it only seems fair that they get some recognition for their contributions. And "real pilots" will still insist that they not share the same medal with drone operators. As one Air Force colonel told Politico last year, The basic fact of the matter is no one is shooting back at you. That makes a big difference. Combat pilots respect drone pilots, but I think we d be uneasy about it if they were to get the same award.

There were rumblings about a new award as early as last summer, and now it appears to be a #SlatePitch come to life. The Distinguished Warfare Medal would be the first combat-award created by the Armed Forces since World War II, and would become the fourth-highest ranking combat decoration. (It would rank above the Bronze Star, but below the Silver Star.) Defense Secretary Leon Panetta may announce the new medal as soon as today.

Spain Busts 'Ransomware' Cybercrime Gang

Spanish authorities on Wednesday announced the breakup of a cybercrime gang that used a "ransomware" virus to lock computers throughout Europe, display false messages claiming the action was taken by police and demand payment of 100 ($135) to unlock the computers.

The gang, operating from the Mediterranean resort cities of Benalmadena and Torremolinos, made at least 1 million ($1.35 million) annually, said Deputy Interior Minister Francisco Martinez. Their notices to victims were accompanied by false threats claiming they were under investigation for accessing child pornography or illegal file-sharing.

The 27-year-old Russian alleged to be the gang's founder and virus developer was detained in the United Arab Emirates at the request of Spanish police while on vacation and an extradition petition is pending, Martinez said. Six more Russians, two Ukrainians and two Georgians were arrested in Spain last week.

Europol, which coordinates national police forces across Europe and worked with Spanish authorities on the case, said the operation "dismantled the largest and most complex cybercrime network dedicated to spreading police ransomware."

Europol, based in The Hague, Netherlands, added that the gang infected tens of thousands of computers worldwide, and Spanish authorities said people from 30 mostly European nations were affected.

"It's an example of the evolving nature of cybercrime online," Europol director Rob Wainwright said. "It's an example of how cybercriminals are

becoming more sophisticated in affecting thousands of people around Europe."

The virus displayed the national emblem of the police force in each country it appeared, telling people to buy prepaid electronic money cards to pay the fines online.

Authorities estimate less than 3 percent of those people whose computers were infected paid, but the amounts added up. The gang also stole data and information from victims' computers, and didn't unlock them after the fake fines were paid.

Money was also stolen from the victims' accounts via ATMs in Spain, and the gang made daily international money transfers through currency exchanges and call centers to send the funds stolen to Russia.

Spanish authorities identified more than 1,200 victims but said the actual number could be much higher. The government's Office of Internet Security received 784,000 visits for advice on how to get rid of the virus.

Those arrested face charges of money laundering, participation in a criminal operation and fraud.

Facebook Says It Was Hacked

Facebook said on Friday that it been the target of a series of attacks by an unidentified hacker group, but it had found no evidence that user data was compromised.

"Last month, Facebook security discovered that our systems had been targeted in a sophisticated attack," the company said in a blog post. "The attack occurred when a handful of employees visited a mobile developer website that was compromised."

The social network, which says it has more than one billion active users worldwide, added: "Facebook was not alone in this attack. It is clear that others were attacked and infiltrated recently as well."

Facebook's announcement follows recent cyber attacks on other prominent websites. Twitter, the microblogging social network, said this month that it had been hacked, and that approximately 250,000 user accounts were potentially compromised, with attackers gaining access to information including user names and email addresses.

Newspaper websites including The New York Times, The Washington Post, and The Wall Street Journal have also been infiltrated, according to the news organizations. Those attacks were attributed by the news organizations to Chinese hackers targeting their coverage of China.

Valentine's Day Scammers Go for the Heart

Not every Valentine's Day message is as sweet as it may appear.

With the year's most romantic day just around the corner, spammers are

taking advantage of both singles and couples with "find your Valentine" spam email and too-good-to-be-true discounts on jewelry, nightlife and other items.

In one particular scam that computer security firm Symantec reported on its blog, victims are infected after opening a malicious ZIP file.

In another, victims are given a bogus discount code and lured into clicking to a page that requests sensitive personal and financial information to be used to commit fraud or ID theft at a later date.

Scammers are infecting singles, too. They know that if you're not shopping for that special someone, you're probably looking for him or her.

Scammers tug on singles' heartstrings with messages from "your secret crush" and the like. They hope to infect computers with malicious email attachments or to direct potential victims to Web pages where private details are demanded.

Dangers lurk outside of Internet users' email inboxes as well. Those seeking a live human connection in an online chatroom could be duped by a "chatbot" into thinking they're talking to a real person.

With a little bit of preprogrammed flirtatiousness, a machine can gain a user's trust and direct him or her to sites that could infect machines with malware, or lure users into entering financial and personally identifiable information.

By that same token, fake online dating profiles have proven to be an effective method of gaining a victim's trust and extracting personal details. Victims can and have had their identities stolen and have even been blackmailed.

The old adage still applies: If it sounds too good to be true, it probably is. Consumers need to be wary of unsolicited messages that promise deep discounts and skeptical of any page that asks for sensitive information.

No matter how lonely or how much users long for love as Valentine's Day approaches, it's important not to let those feelings get in the way of safely surfing the Internet.

A computer virus is much more difficult, and a lot less fun, to remove than a lipstick-laden smooch on the cheek.

Egyptian Regulator Appeals Against Court's YouTube Ban

Egyptian authorities appealed on Thursday against a court order banning the video file-sharing site YouTube for a month over an amateur video that denigrates the Prophet Mohammad, saying the ruling was unenforceable.

"The National Telecommunication Regulatory Authority has presented an appeal to halt implementation of the verdict," said a statement from the Ministry of Communications and Information Technology.

Egypt's administrative court ordered the ministries of communication and investment to block YouTube, owned by Google, inside the country because it had carried the film "Innocence of Muslims", said the state news agency

MENA.

The low-budget 13-minute video, billed as a film trailer and made in California with private funding, provoked a wave of anti-American unrest in Egypt, Libya and dozens of other Muslim countries in September.

The video depicts the Prophet as a fool and a sexual deviant. For most Muslims, any portrayal of the Prophet is considered blasphemous.

A statement issued after talks between ministry officials and the telecoms regulator said it was technically impossible to shut down YouTube in Egypt without affecting Google’s Internet search engine, incurring potentially huge costs and job losses.

"The government cannot carry out the contents of the verdict within Egypt’s borders," the statement said. The only step the authorities could take was to block the offending film within Egypt, which had already been done.

Only the United States had the capability to shut down YouTube, it said.

"Blocking YouTube would affect the search engine of Google, of which Egypt is the second biggest user in the Middle East," the statement said. This would cause losses to the economy of up to hundreds of millions of Egyptian pounds (tens of millions of dollars) and affect thousands of jobs, it added.

In a statement, Google said it had created a simple mechanism for legal authorities to request the blocking of content viewed as illegal.

Adobe Reviews Report of Another Security Bug in Its Software

Adobe Systems Inc is investigating a report by a cybersecurity firm that hackers exploited previously unknown bugs in its Reader and Acrobat software to launch sophisticated attacks on personal computers.

FireEye, a Silicon Valley company that helps businesses fight cyber attacks, told Reuters it obtained so-called PDF files tainted with malicious software, which can take advantage of the newly discovered bugs.

It declined to identify any victims of the attacks.

A spokeswoman for Adobe said that the company is investigating the report, which surfaced late on Tuesday. She declined to elaborate.

This has been a busy year so far for Adobe’s security team. In January, the company pushed out security updates to fix vulnerabilities in Reader, Acrobat and Flash, as well as a program known as ColdFusion that is used to build websites.

Last week, it rushed out a fix for Flash Player after security software maker Kaspersky Lab identified a critical bug that enabled hackers to install "back doors" and take control of PCs running on Microsoft Corp’s Windows operating system or Apple Inc’s Mac OS X.

Adobe’s software has long been a popular target for hackers, who attack PCs by finding bugs in widely used programs that they can then exploit to

insert viruses on computers. Experts estimate that Reader and Acrobat programs for accessing PDF documents and Flash Player for accessing Internet content are installed on more than 1 billion PCs.

Hackers exploiting the most recently discovered vulnerability use PDF files to infect PCs, according to FireEye.

When the victim opens the PDF, a visa application form appears onscreen, and a virus installs a covert communications channel with a remote computer known as a "command and control" server, which hackers use to control infected PCs, said Zheng Bu, senior director of research at FireEye.

He said the virus also installs a third malicious file on the infected computer, but declined to elaborate.

Adobe has yet to provide advice on how to protect PCs against attack. FireEye said computer users should avoid opening unfamiliar PDFs, especially when coming from unknown sources.

FireEye said on its blog it has observed attacks on PCs running Adobe Reader 11, the most-recent version of the software, as well as Reader 9 and Reader 10.

Adobe said on its own security blog that the issue also affected Acrobat XI, the current version of the software used to create PDF documents.

Employee Facebook Privacy Bill Advances in Colorado

Facebook profiles and other social-media accounts could be off-limits to employers under a bill approved unanimously in a Colorado House committee Tuesday.

The measure, approved 11-0, would bar most employers from requiring access to their workers’ personal accounts. Several states already have such protections, and dozens more are considering them.

The bill would not prohibit companies from looking at Facebook pages or punishing employees for what they post on their personal sites. But it would ban them from requiring current or potential employees to provide passwords for personal accounts.

The measure’s sponsor said private social media accounts should be considered like physical photographs.

"It’s never been acceptable for en employer to ask to see an employee’s personal photos," said Rep. Angela Williams, D-Denver.

The bill was amended to exempt law enforcement agencies and corrections workers, since those workers’ personal opinions or off-duty actions can affect their use as witnesses in criminal matters.

"They need to know that the people they have working for them are above reproach and have a higher standard," said Ann Marie Jensen of the Colorado Association of Chiefs of Police.

Lawmakers rejected a proposal to give all businesses permission to require

personal social media access for "legitimate business interests."

Kim Smiley of the Colorado Defense Lawyers Association suggested businesses should be allowed to require access in some cases. She used examples of an employee threatening violence or bragging about drinking alcohol on the clock.

Lawmakers responded that employers dealt with those problems long before social media networking. Rep. Libby Szabo, R-Arvada, pointed out that employers once used their noses to suss out an employee who drank too much at lunch.

"There was life before Facebook," Szabo said.

The measure awaits one more committee vote before it’s considered by the full House.

NH Bills: Bosses Can’t Seek Social Media Passwords

New Hampshire is considering joining a handful of states that bar employers from asking job applicants and employees for their social media user names and passwords.

The House’s labor committee is holding a hearing on two similar bills Tuesday that would prohibit an employer from requiring the disclosure. Maryland, California, Delaware, Michigan, New Jersey and Illinois have similar laws and two dozen besides New Hampshire are considering legislation, according to the National Conference of State Legislatures.

In their effort to vet job applicants, some companies and government agencies have started asking for passwords to log into a prospective employee’s accounts on social media sites, such as Facebook and Twitter. Critics call it an invasion of privacy akin to handing over the keys to the person’s house.

State Sen. Donna Soucy, a co-sponsor on both New Hampshire bills, said Monday that employers can gain access to information about an employee or job applicant through social media accounts like Facebook that they otherwise could not legally obtain. She said people post personal information about themselves on Facebook or others post on the person’s page that should be protected.

She said she has not heard of any New Hampshire employers demanding the information.

"I think the issue is something we need to consider a lot more seriously than we used to" with the growth of social media accounts, she said. "At the very least, I would hope we would have a study."

Soucy, D-Manchester, said employers can use information on social media accounts to discriminate. For example, the applicant might be obese but the person’s weight would not be required on the application. The employer might not know until seeing a picture on Facebook, she said.

"Would they interview them if they saw their picture on Facebook?" she said.

Soucy said other people can post information on the person’s page that the person might not delete before a prospective employer saw it.

"As responsible as somebody might trying to be, it is still a reflection on them," she said.

Allowing employers access to social media accounts also gives them access to others linked to the account at the infringement on their privacy, she said.

Google Under Fire for Sending Users’ Information to Developers

Sebastian Holst makes yoga mobile apps with his wife, a yoga instructor.

The Mobile Yogi is sold in all the major mobile app stores. But when someone buys his app in the Google Play store, Holst automatically gets something he says he didn’t ask for: the buyer’s full name, location and email address.

He says consumers are not aware that Google Inc. is sharing their personal information with third parties. No other app store transmits users’ personal information to third-party developers when they buy apps, he said.

"Google is not taking reasonable steps to ensure that this data is used correctly," said Holst, whose app has 120,000 users.

Google is coming under fire just as regulators in the U.S. and overseas are stepping up their scrutiny of how all the players in the industry - mobile apps, stores, advertising networks and others - handle consumers’ private information. Regulators are pushing for greater transparency of what information is collected by apps and how it’s shared.

Google Play has worked differently than Apple Inc.’s iTunes since it launched in October 2008. An app developer sets up an account through the mobile payment system Google Wallet, which makes them a merchant in the store. When someone buys his or her app from Google Play, that transaction - and the customer’s information - is sent to the developer. The developer has to comply with rules about what he or she can do with the information.

But at Apple, iTunes is the merchant. App developers say they never receive customer information.

Google defended how Google Play operates in an emailed statement.

"Google Wallet shares the information necessary to process a transaction, which is clearly spelled out in the Google Wallet Privacy Notice," Google said.

Barry Schwartz, Search Engine Land’s news editor, said he prefers it that way.

"I want to be able to service my customers, and yes, they are my customers, not Google s and not Apple s customers. They download our products. They call the developer with questions. We provide them the tools and the content. They are our customers, Schwartz wrote in a blog post. "Apple doesn’t tell us who our customers are, and when we need that

information to verify ownership or to give refunds, we are left with blindfolds on. Google, in my opinion, does it right by making the user who downloads the app our customer."

But Danny Sullivan, founding editor of Search Engine Land, said Google should make it clear to consumers that their information is being shared with third-party developers.

"Google's privacy policies don't make clear this is happening, something Google probably needs to correct," Sullivan said. "I sure had no idea that Google Play did this."

Nor did Dan Nolan, an Australian app developer. He said he was astonished when he found out that Google was sending him users' names, email addresses, city and ZIP Code. He wrote a blog post Wednesday condemning Google for doing it.

Nolan runs a popular app in Australia called the Paul Keating Insult Generator that throws out quips worthy of the former labor prime minister there.

"Under no circumstances should I be able to get the information of the people who are buying my apps unless they opt into it and it's made crystal clear to them that I m getting this information," Nolan said.

Privacy watchdogs say consumers are largely in the dark that Google is sending their information to outside developers despite assurances from Google that it tells them when they sign up for Google Wallet. That, they say, is "troublesome."

"The question is: What constitutes meaningful consent?" said Marc Rotenberg, executive director of the Electronic Privacy Information Center. "The bottom line is that users are not able to control how their data is being gathered and disclosed."

Apple may have started the mobile app boom in 2008, but Google is catching up. As of October, Google Play had the same number of apps - 700,000 - as Apple.

Google is trying to press its advantage by making it easier for developers to build apps and easier for users to buy them. Apps help fuel the growing popularity of phones that run Google's Android software. Apple s app sales still generate several times the revenue of Google's.

Google does not run its app store with the same ironclad control that Apple does, and that has occasionally led to problems.

It's also had run-ins with federal regulators over privacy. Google agreed in 2011 that it would ask users before sharing their data with outsiders to settle government claims that it violated its users' privacy with its social network Buzz.

The Federal Trade Commission settlement also required the search giant to submit to independent privacy audits every two years for 20 years. Last year Google had to pay $22.5 million to settle charges for bypassing the privacy settings of millions of Apple users. It was the largest penalty ever levied on a company by the FTC.

Google is not the only company to come under fire for how it shares information with app developers. In 2011, Facebook Inc. agreed to a 20-year

privacy settlement with the FTC that required the company to get users' permission before changing the way it treats personal information. The FTC alleged that Facebook engaged in deceptive behavior when it promised that third-party apps would only have access to user information they needed when in fact many apps had unrestricted access to users' personal data.

Facebook Wins German Court Fight on Fake Names Ban

Facebook has won a court battle against a German privacy watchdog that challenged the social networking site's policy requiring users to register with their real names.

Schleswig-Holstein state's data protection body said Friday it will appeal the court decision. It argues the ban on fake names breaches German privacy laws and European rules designed to protect free speech online.

The administrative court in northern German Schleswig argued in its ruling Thursday that German privacy laws weren't applicable because Facebook has its European headquarters in Ireland which has less far-reaching rules.

The California-based company argues its real name policy protects users.

Germany's strict privacy rules have posed a legal headache for Facebook, Google and others in recent years, giving consumers significant rights to limit the way companies use their information.

Raytheon's 'Google for Spies' Tracks You from Social-Media Sharing

As if you weren't paranoid enough about your Facebook privacy settings, now your ever social-media move can be mined for the purposes of actual spying. The Guardian has lifted the veil on RIOT, an as-yet-unsold program from defense contractor Raytheon that looks through Facebook, Twitter, Gowalla, and Foursquare to find out where a person lives and hangs out, to discover what he or she looks like, and even to predict what he or she will do in the future. With the secret program officially named Rapid Information Overlay Technology it took Raytheon's "principal investigator" ess than a minute to put together this map of where one man travels:

As much of a privacy overstep as this appears to be, it's totally legal because we're the ones sharing the information on the public Internet. Just a year ago the FBI put out a call, looking for a "social media alert mapping and analysis application solution," according to a request for information (RFI) posted on FedBizOpps.gov. The United Kingdom has also indicated similar interests. Ratheon hasn't sold the technology to any of its clients, but the world's fifth largest defense contractor said it worked with the U.S. government in 2010 on the Riot project.

For obvious reasons, privacy experts think the program presents some possible privacy violations. "Social networking sites are often not transparent about what information is shared and how it is shared," the Electronic Privacy Information Center's Ginger McCall told The Guardian's Ryan Gallagher. "Users may be posting information that they believe will

be viewed only by their friends, but instead, it is being viewed by government officials or pulled in by data collection services like the Riot search." With data-mining tools, making people uncomfortable can count as a privacy violation, as we have seen with other oversteps taken by Facebook.

In any case, this might be a good time to ensure those Facebook privacy settings are locked down. If you change your sharing settings from public to custom or "friends," per the picture at right that might help keep private contractors off your digital trail. Or, as always, the best way to avoid unwanted tracking is to abstain from Internet sharing altogether.

Facebook Graph Search To Shield Minors

Facebook's Graph Search, which was released to a limited number of users in January, allows people to more easily search the social network. The feature makes it much easier to find out information about friends - "Movies my friends like" - and easier to find your friends or people on the service - for example, "people who live in New York under the age of 25."

The feature, while very useful, does raise security and privacy issues, which we noted right after it was released. Facebook has said that the search tool follows the service's privacy settings, and today Facebook clarified that there are built-in privacy and security features to shield younger users specifically.

"As with all of our products, we designed Graph Search to take into account the unique needs of teens on Facebook," Facebook's safety team wrote in a blog post today. You must be 13 or older to use Facebook, according to the services Terms and Conditions, and says this applys to those between the ages of 13 and 17.

Facebook says teens will be protected based on current restrictions and settings for teens. Currently teens can only share information with "friends" or "friends of friends"; they cannot share it with the "public" setting, which goes out to anyone with a Facebook account.

Beyond that, Facebook has constructed Graph Search in a way that limits adults who are "friends of friends" to find a younger person.

"In addition, for certain searches that could help to identify a young person by age or by their location, results will only show to that person's Friends, or Friends of Friends who are also between the age of 13-17," Facebook explains.

We'll make that a bit easier for you to understand. Say 14-year-old Jessica is friends with 13-year-old Mary and both of them live in Los Angeles. Now say, Jessica is friends with John, a 30-year old man. If John searched "People under the age of 15 who live in Los Angeles" through Graph Search Mary wouldn't show up. Jessica would since he is friends with her.

The settings aim to prevent adults from easily finding younger people on the service. Facebook also restricted sex offenders from using the service. "You will not use Facebook if you are a convicted sex offender," Facebook states in its terms and conditions.

In today’s blog post, Facebook also suggests some other safety tips for Graph Search. It suggests that you be aware of who you are sharing your photos, statues and other information with. Additionally, keep an eye on your Activity Log, which lets you see who you have shared your information with.

Facebook still hasn’t said when it will begin rolling out Graph Search to a wider audience. Users can request the feature at www.facebook/graphsearch.

Apple Cuts MacBook Pro Price, Updates Processors

Apple says it has lowered the price of its 13-inch MacBook Pro laptops by $200 and updated its processors. It also launched new models with faster processors and more memory.

Apple Inc. said Wednesday that the MacBook Pro with "Retina" display and 128 gigabytes of flash memory will now cost $1,499, down from $1,699. A new model with 256 gigabytes of flash will cost $1,699.

The 15-inch model has a faster processor and the same price.

Apple unveiled the new MacBook Pro models last fall. It has flash memory instead of the traditional hard drive, which makes it thinner and lighter.

Apple reported a surprising decline in Mac sales in the final quarter of 2012. It sold 4.1 million of them, down 22 percent from shipments a year earlier.

Finally Invented: A Computer Incapable of Crashing

Good news for folks who regularly find themselves mashing control+alt+delete until their fingernails hurt: Researchers at the University College London have invented a new "systemic" computer that automatically repairs corrupted data whenever it appears. In non-geek speak, all that means is that this gilded, Platonic ideal of desktop PCs never, ever crashes.

How does such a miracle machine even work? Its creators, naturally, turned to Mother Nature more specifically, the random modeling that allows swarms of bees to scatter in unison around a honey-hungry bear or that allows atoms to bounce around until they find their proper place.

"Today’s computers work steadily through a list of instructions: One is fetched from the memory and executed, then the result of the computation is stashed in memory," explains Paul Marks at New Scientist. Crashes happen when a computer mangles these kinds of linear instructions and the code doesn’t quite know what to do next. Hence, the dreaded error message. The new computer works a bit differently, dividing instructions into little digital slots called "systems." Here, an explanation:

Each system has a memory containing context-sensitive data that means it

can only interact with other, similar systems. Rather than using a program counter, the systems are executed at times chosen by a pseudorandom number generator, designed to mimic nature's randomness. The systems carry out their instructions simultaneously, with no one system taking precedence over the others.

That means whenever a chunk of data hits a wall, these randomly-generated paths simply reroute these instructions through various systems (all containing the same message) to help it accomplish its original goal without shutting down. Kind of, but not exactly like how the human brain is capable of rewiring its neural pathways around obstructions. The creators of the device are optimistic, and think this intelligent, self-repairing tech could one day help damaged drones reprogram themselves on the fly, enable bioengineers to create more realistic models of the human brain, and trigger sentience in emerging mainframes like SkyNet. (One of these isn't for real.) The team plans on presenting their findings at a conference in Singapore this April.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.